Probabilité d'engendrer le groupe symétrique avec un couple de permutations : la conjecture de Netto

Pierre Besson
TER de M1 encadré par Tanguy Rivoal

27 juin 2025

Table des matières

1 Introduction

Prenons un couple de permutations au hasard dans le groupe symétrique $\mathfrak{S}_n$. Quelle est la probabilité que le groupe engendré avec ces deux permutations soit le groupe symétrique ou le groupe alterné ? En 1893, Netto a conjecturé dans [6, p. 90] que la probabilité d'engendrer le groupe symétrique tend vers $3/4$ quand n tend vers l'infini. Dixon a démontré cette conjecture 76 ans plus tard dans [3] en 1969. Pour cela, il a utilisé des notions de combinatoire classiques mais aussi la théorie des groupes de permutations finis, avec notamment l'utilisation d'un théorème dû à Jordan faisant intervenir les notions de groupes transitifs et groupes primitifs (voir la partie 2 pour les définitions). Dans ce TER, on détaillera donc la preuve faite par Dixon ainsi que celle du théorème de Jordan qu'il invoque dans le but de montrer les théorèmes suivants, vérifiant la conjecture de Netto.

Théorème 1 (Dixon [3]). *La proportion des couples $(x, y) \in \mathfrak{S}_n^2$ qui engendrent un sous-groupe transitif de $\mathfrak{S}_n$ est*

$$1 - \frac{1}{n} + O\Big(\frac{1}{n^2}\Big)$$

lorsque $n \to \infty$. La même estimation asymptotique est valable pour la proportion des couples qui engendrent un sous-groupe primitif de $\mathfrak{S}_n$. Ainsi, un couple d'éléments de $\mathfrak{S}_n$ engendre un sous-groupe primitif environ $n - 1$ fois sur n.

Théorème 2 (Dixon [3]). *La proportion des couples $(x, y) \in \mathfrak{S}_n^2$ qui engendrent soit $\mathfrak{A}_n$ soit $\mathfrak{S}_n$ est supérieure à*

$$1 - \frac{2}{(\log(\log n))^2}$$

pour tout n suffisamment grand.

Le groupe engendré par un couple $(x, y) \in \mathfrak{S}_n^2$ est inclus dans $\mathfrak{A}_n$ si et seulement si x et y sont toutes les deux des permutations paires. Comme la moitié des permutations de $\mathfrak{S}_n$ sont impaires, le corollaire suivant en découle immédiatement et démontre donc la conjecture de Netto.

Corollaire 1 (Dixon [3]). *La probabilité qu'un couple $(x, y) \in \mathfrak{S}_n^2$ engendre $\mathfrak{S}_n$ tend vers $3/4$ lorsque $n \to \infty$. La probabilité qu'un couple $(x, y) \in \mathfrak{A}_n^2$ engendre $\mathfrak{A}_n$ tend vers 1 lorsque $n \to \infty$.*

La suite de ce texte est consacré à la démonstration de ces résultats.

2 Définitions et propriétés importantes

Dans toute cette partie, les définitions et propriétés mentionnées s'appuieront sur les livres [7] et [1].

Définition 1. *Le groupe symétrique $\mathfrak{S}_n$ est le groupe formé par toutes les bijections d'un ensemble à n éléments sur lui-même, c'est-à-dire l'ensemble des permutations de n objets. Il est défini par*

$$\mathfrak{S}_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \sigma \text{ est bijective}\}$$

avec pour loi de groupe la composition des applications.

Quelques propriétés de $\mathfrak{S}_n$.
- L'ordre de $\mathfrak{S}_n$ est $n!$ (le nombre total de permutations possibles).
- $\mathfrak{S}_n$ est un groupe non abélien pour $n \geq 3$.

Définition 2 (Les p-cycles)**.** *Un p-cycle est une permutation qui agit sur p éléments en les envoyant les uns sur les autres de manière circulaire, tandis que les autres éléments restent inchangés. On le note sous la forme*

$$\sigma = (a_1\ a_2\ \ldots\ a_p).$$

L'ordre d'un p-cycle est p, car il faut p applications successives de σ pour retrouver l'identité.

Les cycles jouent un rôle fondamental dans la décomposition des permutations : toute permutation peut être écrite comme un produit de cycles disjoints (c'est-à-dire concernant des ensembles distincts d'éléments).

Définition 3 (Signature d'une permutation)**.** *La signature (ou parité) d'une permutation σ est la fonction*

$$\varepsilon(\sigma) = (-1)^k,$$

où k est le nombre minimal de transpositions nécessaires pour écrire σ. Si k est pair, alors $\varepsilon(\sigma) = +1$ et σ est dite paire. Si k est impair, alors $\varepsilon(\sigma) = -1$ et σ est dite impaire.

Un p-cycle a pour signature

$$\varepsilon((a_1\ a_2\ \ldots\ a_p)) = (-1)^{p-1}$$

car il peut être écrit comme le produit de $p-1$ transpositions et c'est le plus petit nombre possible.

La signature est un homomorphisme de groupes de $\mathfrak{S}_n$ vers le groupe multiplicatif $\{\pm 1\}$, dont le noyau est précisément $\mathfrak{A}_n$.

Définition 4 (Le groupe alterné $\mathfrak{A}_n$)**.** *Le groupe alterné $\mathfrak{A}_n$ est le sous-groupe de $\mathfrak{S}_n$ formé des permutations paires, c'est-à-dire celles qui peuvent être décomposées en un nombre pair de transpositions. Il est défini par*

$$\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \varepsilon(\sigma) = +1\}.$$

Quelques propriétés de $\mathfrak{A}_n$.
- $\mathfrak{A}_n$ est un sous-groupe normal de $\mathfrak{S}_n$.(Voir la définition 13 ci-dessous)
- Son ordre est $|\mathfrak{A}_n| = n!/2$.
- Pour $n \geq 5$, $\mathfrak{A}_n$ est un groupe simple, c'est-à-dire qu'il n'a pas de sous-groupes normaux non triviaux.

Définition 5 (Partitions d'un ensemble)**.** *Une partition d'un ensemble à n éléments est une décomposition de cet ensemble en sous-ensembles disjoints non vides dont l'union reconstitue l'ensemble initial.*

Formellement, une partition d'un ensemble E de n éléments est une famille de sous-ensembles $\{E_1, E_2, \ldots, E_k\}$ telle que :

(i) $E_1 \cup E_2 \cup \cdots \cup E_k = E$ *;*

(*ii*) $E_i \cap E_j = \emptyset$ *pour* $i \neq j$;

(*iii*) $E_i \neq \emptyset$ *pour tout* i.

Définition 6 (Action de groupe)**.** *Une action de groupe est une application*

$$\phi : G \times X \to X$$

qui associe à chaque élément $g \in G$ *et* $x \in X$ *un élément* $\phi(g, x)$*, noté souvent* $g \cdot x$*, et qui satisfait les propriétés suivantes :*

— *Compatibilité avec la loi du groupe :*

$$(gh) \cdot x = g \cdot (h \cdot x), \quad \forall g, h \in G, \quad \forall x \in X.$$

— *Action de l'élément neutre :*

$$e \cdot x = x, \quad \forall x \in X.$$

Exemple : on peut faire agir $\mathfrak{S}_n$ sur $\Omega := \{1, 2, \ldots, n\}$(on reprendra cette notation dans toute la suite) de la manière suivante :

$$\sigma \cdot i = \sigma(i), \quad \forall \sigma \in \mathfrak{S}_n, \quad \forall i \in \Omega.$$

Définition 7 (Groupe engendré)**.** *Soit* S *un sous-ensemble d'un groupe* G *avec une loi que l'on appelle produit. Le sous-groupe engendré par* S *est le plus petit sous-groupe de* G *contenant* S*. Autrement dit, c'est l'ensemble des éléments obtenus en prenant tous les produits finis possibles d'éléments de* S *et de leurs inverses. On le note* $\langle S \rangle$*.*

Exemple : les permutations $\sigma = (1\ 2\ 3)$ et $\tau = (1\ 2)$ engendrent $\mathfrak{S}_3$. En effet,

— $\sigma^2 = (1\ 3\ 2)$;

— $\tau\sigma = (2\ 3)$;

— $\tau\sigma\tau = (1\ 3)$.

Les six éléments de $\mathfrak{S}_3$ peuvent donc s'écrire comme suit en fonction de σ et τ :

$$\begin{aligned} e &= \mathrm{id}, \\ \sigma &= (1\ 2\ 3), \\ \sigma^2 &= (1\ 3\ 2), \\ \tau &= (1\ 2), \\ \tau\sigma &= (2\ 3), \\ \tau\sigma\tau &= (1\ 3). \end{aligned}$$

Ainsi, nous obtenons tous les éléments de $\mathfrak{S}_3$, ce qui montre que $\mathfrak{S}_3 = \langle \sigma, \tau \rangle$.

Définition 8 (Sous-groupe transitif)**.** G *est un sous-groupe transitif d'un groupe* H *pour l'action de* H *sur* X *si l'action de* G *sur* X *est transitive, c'est-à-dire pour chaque couple d'éléments* $(i, j) \in X^2$*, il existe un élément* $g \in G$ *telle que* $g \cdot i = j$*.*

Exemple : $\mathfrak{S}_n$ est évidemment un sous-groupe de $\mathfrak{S}_n$ transitif car $\forall i, j \in [\![1, n]\!], (i\ j) \in \mathfrak{S}_n$ et $(i\ j)(i) = j$. Le groupe

$$\langle (1\ 2), (3\ 4) \rangle = \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

est un sous-groupe non transitif de $\mathfrak{S}_4$, car il ne relie pas $\{1, 2\}$ et $\{3, 4\}$. Le groupe

$$\langle (1\ 2\ 3) \rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

est un sous-groupe transitif de $\mathfrak{S}_3$, car en appliquant (1 2 3), on peut atteindre n'importe quel élément de $\{1, 2, 3\}$.

Définition 9 (Sous-groupe primitif)**.** *Un groupe de permutations G agissant sur un ensemble fini non vide X est dit primitif si G agit transitivement sur X et si les seules partitions préservées par l'action de G sont les partitions triviales : soit l'ensemble entier, soit les $|X|$ singletons. Par ailleurs, si G est transitif et préserve une partition non triviale, alors G est dit imprimitif.*

Remarque : "imprimitif" est différent de "non-primitif" car le premier est transitif et le second pas nécessairement.

Exemple : le groupe $\langle (1\ 2\ 3) \rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$ est un sous-groupe primitif de $\mathfrak{S}_3$ car il est transitif et id, (1 2 3) et (1 3 2) ne préservent aucune partition non triviale.

Le groupe $\langle (1\ 2\ 3\ 4) \rangle$ est quant à lui un sous-groupe imprimitif de $\mathfrak{S}_4$ car il est transitif mais la partition de $[\![1, 4]\!]$ en $X_1 = \{1, 3\}$, $X_2 = \{2, 4\}$ est préservée par (1 2 3 4). En effet, on a que $(1\ 2\ 3\ 4)(X_1) = X_2$ et $(1\ 2\ 3\ 4)(X_2) = X_1$, donc quel que soit $n \in 2\mathbb{Z}$, $(1\ 2\ 3\ 4)^n(X_1) = X_1$ et $(1\ 2\ 3\ 4)^n(X_2) = X_2$ et quel que soit $n \in 2\mathbb{Z} + 1$, on a $(1\ 2\ 3\ 4)^n(X_1) = X_2$ et $(1\ 2\ 3\ 4)^n(X_2) = X_1$.

Définition 10 (Groupe k-transitif)**.** *Un groupe G agissant sur un ensemble X est dit k-transitif si pour tout couple de k-uplets $(x_1, \ldots, x_k)$ et $(y_1, \ldots, y_k)$ d'éléments distincts de X, il existe un élément $g \in G$ tel que $g \cdot x_i = y_i$ pour tout $1 \leq i \leq k$. On remarquera que k+1-transitif implique k-transitif.*

Par exemple,

— Le groupe symétrique $\mathfrak{S}_n$ est n-transitif.

— Le groupe alterné $\mathfrak{A}_n$ est $(n-2)$-transitif pour $n \geq 5$.

Définition 11 (Groupe k-primitif)**.** *Un groupe G est k-primitif sur Ω si les sous-groupes de G qui laissent $k-1$ points de Ω fixés sont primitifs sur le reste de Ω.*

Définition 12 (Sous-groupe de Sylow)**.** *Soit G un groupe fini, et soit p un nombre premier. Un sous-groupe de p-Sylow de G est un sous-groupe $P \leq G$ d'ordre p^n (la notation "$\leq$" désignant le fait d'être un sous-groupe).*

Définition 13 (Sous-groupe normal)**.** *Un sous-groupe $N \leq G$ est dit normal si pour tout $g \in G$, on a $gNg^{-1} = N$. On note $N \trianglelefteq G$ et on note $N(G)$ le normalisateur de G, c'est le plus grand sous-groupe normal de G.*

Par exemple,
- $\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$.
- Le centre $Z(G)$ est toujours normal dans G.

Définition 14 (Sous-groupe dérivé)**.** *Le sous-groupe dérivé d'un groupe G, noté $[G, G]$, est le sous-groupe engendré par les commutateurs $[g, h] = ghg^{-1}h^{-1}$ pour $g, h \in G$. Ce groupe est un sous-groupe normal de G.*

Par exemple,
- Si G est abélien, alors $[G, G] = \{1_G\}$.
- $[\mathfrak{S}_n, \mathfrak{S}_n] = \mathfrak{A}_n$.

Définition 15 (Bloc)**.** *Pour G un groupe de permutations sur Ω on appelle un sous-ensemble Δ de Ω un bloc de G si pour tout $g \in G$, $g(\Delta) = \Delta$ ou $g(\Delta)$ n'a aucun point en commun avec Δ.*

Définition 16 (Groupe régulier)**.** *Un groupe G de permutations sur Ω est dit semi-régulier si pour tout $\alpha \in G$, $G_\alpha = 1$. Si G est semi-régulier et transitif sur Ω alors G est dit régulier.*

3 Démonstration du théorème 1

Nous allons démontrer ce théorème en deux étapes.

3.1 Première étape

Soit t_n la proportion des $(n!)^2$ couples $(x, y) \in \mathfrak{S}_n^2$ qui engendrent un sous-groupe transitif de $\mathfrak{S}_n$ et soit p_n la proportion correspondante de celles qui engendrent un sous-groupe primitif de $\mathfrak{S}_n$.

Rappelons que l'on notera $\Omega = \{1, 2, \ldots, n\}$. Pour chaque partition $\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_k$ en sous-ensembles disjoints, le nombre de couples $(x, y) \in \mathfrak{S}_n^2$ tels que le groupe engendré possède précisément $\Omega_1, \Omega_2, \ldots, \Omega_k$ comme orbites est égal à

$$\prod_{i=1}^{k} (n_i!)^2 t_{n_i},$$

où $n_i = |\Omega_i|$ $(i = 1, 2, \ldots, k)$. En effet, nous pouvons choisir les couples $(x|\Omega_i, y|\Omega_i)$ (avec $x|\Omega_i$ qui deésigne la restriction de x à Ω_i) indépendamment pour chaque i sous la seule condition que $(x|\Omega_i, y|\Omega_i)$ engendre un groupe transitif sur Ω_i. Une permutation de $\mathfrak{S}_n$

vérifiant cela se construit donc avec les permutations qui engendrent un sous-groupe transitif de $\mathfrak{S}_{n_i}$; il y en a donc $(|\Omega_i|!)^2 t_{|\Omega_i|} = (n_i!)^2 t_{n_i}$. De plus, le nombre de façons de partitionner Ω en k_i ensembles de cardinal i (tels que $\sum_{i=1}^{n} ik_i = n$) est donné par

$$v_{k_1 k_2 \dots k_n} = \frac{n!}{\prod_{l=1}^{n} (i!)^{k_i} k_i!}.$$

En effet le nombre de façon de créer des partitions ordonnées pour un ensemble à n éléments est donné par le coefficient multinomial $\binom{n}{n_1\ n_2\ \dots\ n_k} = \frac{n!}{\prod_{i=1}^{k} n_i!}$ ([2, p.43]). Or ici l'ordre des ensembles qui réalisent la partition n'a pas d'importance. On peut donc considérer les partitions comme ordonnées mais seulement pour les ensembles de cardinaux différents, les autres étant indiscernables. Avec le coefficient multinomial on en a donc compté $\prod k_i!$ fois le nombre de partitions comme souhaité. On a donc avec ce qui a été fait précédemment que

$$\begin{aligned} |\mathfrak{S}_n|^2 = (n!)^2 &= \sum v_{k_1 k_2 \dots k_n} \prod_{i=1}^{n} \left((i!)^2 t_i \right)^{k_i} \\ &= n! \sum \prod_{i=1}^{n} \frac{(i! t_i)^{k_i}}{k_i!}, \end{aligned}$$

où les deux sommes portent sur tous les n-uplets $(k_1, k_2, \dots, k_n)$ pour lesquels chaque k_i est un entier ≥ 0 et $\sum ik_i = n$. En divisant dans l'équation par $n!$ puis en multipliant par X^n et en sommant sur n, on obtient alors l'égalité suivante sur les séries formelles :

$$\begin{aligned} \sum_{n=0}^{\infty} n! X^n &= \sum_{n=0}^{\infty} X^n \sum_{\sum ik_i = n} \left(\prod_{i=1}^{n} \frac{(i! t_i)^{k_i}}{k_i!} \right) = \prod_{i=1}^{\infty} \left(\sum_{k=0}^{\infty} \frac{(i! t_i)^k}{k!} X^{ik} \right) \text{ (par produit de Cauchy)} \\ &= \prod_{i=1}^{\infty} \exp(i! t_i X^i) = \exp\big(\sum_{i=1}^{\infty} i! t_i X^i \big). \end{aligned}$$

Par différentiation formelle, on a donc

$$\sum_{n=1}^{\infty} n! n X^{n-1} = \left(\sum_{i=1}^{\infty} i! i t_i X^{i-1} \right) \exp\left(\sum_{i=1}^{\infty} i! t_i X^i \right) = \left(\sum_{i=1}^{\infty} i! i t_i X^{i-1} \right) \left(\sum_{n=0}^{\infty} n! X^n \right).$$

Ainsi, en identifiant les coefficients de X^{n-1}, on obtient

$$n = \frac{1}{n!} \sum_{i=1}^{n} i!(n-i)! i t_i = \sum_{i=1}^{n} \frac{i t_i}{\binom{n}{i}}. \tag{1}$$

On peut maintenant utiliser l'équation (1) pour calculer les valeurs de t_n récursivement. Les premières valeurs sont

$$t_1 = 1, \quad t_2 = \frac{3}{4} = 0.75, \quad t_3 = \frac{13}{18} \approx 0.722, \quad t_4 = \frac{71}{96} \approx 0.738$$

$$t_5 = \frac{461}{600} \approx 0.766.$$

Utilisons l'équation (1) pour prouver la première moitié du Théorème 1 :

$$t_n = 1 - \frac{1}{n} + O\Big(\frac{1}{n^2}\Big) \quad \text{lorsque } n \to \infty.$$

Posons $r_n = n(1 - t_n)$. Alors $r_n \geq 0$ puisque $t_n \leq 1$. Nous devons montrer que

$$r_n - 1 = O\left(\frac{1}{n}\right).$$

À partir de (1), nous avons

$$n = \sum_{i=1}^{n} \frac{i}{\binom{n}{i}}\Big(1 - \frac{r_i}{i}\Big) = \sum_{i=1}^{n-1} \frac{(i - r_i)}{\binom{n}{i}} + n - r_n.$$

Donc :

$$r_n = c_n - \sum_{i=1}^{n-1} \frac{r_i}{\binom{n}{i}}, \tag{2}$$

où

$$c_n = \sum_{i=1}^{n-1} \frac{i}{\binom{n}{i}}.$$

Comme pour tout $i \in [\![0, n]\!]$, on a

$$\binom{n}{i} = \binom{n}{n-i},$$

on en déduit que

$$2c_n = \sum_{i=1}^{n-1} \frac{1}{\binom{n}{i}} i + \sum_{i=1}^{n-1} \frac{n-i}{\binom{n}{n-i}} = n \sum_{i=1}^{n-1} \frac{1}{\binom{n}{i}}.$$

Donc pour $n \geq 6$,

$$c_n = \frac{n}{2} \sum_{i=1}^{n-1} \frac{1}{\binom{n}{i}} = 1 + \frac{2}{n-1} + \frac{n}{2} \sum_{i=1}^{n-3} \frac{1}{\binom{n}{i}},$$

comme $i \mapsto \binom{n}{i}$ est croissant sur $[\![1, \lfloor \frac{n}{2} \rfloor]\!]$ et par symétrie autour de $n/2$, nous avons pour $n \geq 6$ que

$$\binom{n}{3} \leq \binom{n}{i} \quad \text{lorsque } 3 \leq i \leq n-3.$$

Par conséquent, le dernier terme dans l'expression de c_n vaut au plus

$$\frac{n}{2\binom{n}{3}}(n-2) = \frac{n(n-2)3!}{2n(n-1)(n-2)} = O\left(\frac{1}{n}\right).$$

Ainsi, $c_n = 1 + O(\frac{1}{n})$ lorsque $n \to \infty$. Enfin, comme $r_i \geq 0$ pour tout i, l'équation (2) montre que $r_i \leq c_i$ et donc $r_i = O(1)$ lorsque $i \to \infty$.

En appliquant (2) à nouveau, on obtient que :

$$r_n = c_n - O\Big(\sum_{i=1}^{n-1} \frac{1}{\binom{n}{i}}\Big) = c_n + O\big(\frac{c_n}{n}\big) = 1 + O\Big(\frac{1}{n}\Big) \quad \text{lorsque } n \to \infty.$$

On peut faire cela car la constante implicite dans le $O(1)$ dans la somme est indépendante de n.

Cela conclut la preuve de la première partie du théorème 1.

3.2 Deuxième étape

Pour la deuxième étape de la démonstration du théorème 1 nous allons d'abord devoir énoncer, ci-dessous, quelques propriétés sur les groupes transitifs et les groupes primitifs.

À tout sous-groupe engendré par un couple de permutations $(x, y) \in \mathfrak{S}_n^2$, on peut associer la partition de $\Omega = [\![1, n]\!]$, $\Omega = \Gamma_1 \cup \Gamma_2 \cup \cdots \cup \Gamma_m$ qui est la partition préservée par l'action du groupe. On remarque aussi que chaque Γ_i est de même cardinal $d = \frac{n}{m}$. En effet l'action du groupe est transitive donc par définition on a forcément que pour tout Γ_i il existe Γ_j tel que Γ_i est l'image de Γ_j par une permutation du groupe. Ces ensembles sont donc en bijection et ont même cardinal. On remarque ensuite que comme pour chaque $\alpha \in \Gamma_i$, les images de α par x et y sont respectivements dans $x(\Gamma_i)$ et $y(\Gamma_i)$. Donc, comme $\langle x, y\rangle$ agit transitivement sur la partition en m blocs, on a que le nombre de couples qui engendrent un sous-groupe primitif qui a pour blocs fixés la partition $\Gamma_1, \Gamma_2, \ldots \Gamma_m$ est au plus

$$(m!)^2 t_m (d!)^{2m}. \tag{3}$$

En effet le nombre de couples de permutations qui engendrent un sous-groupe transitif de $\mathfrak{S}_n$ est $(m!)^2 t_m$ et on construit ensuite les permutations en choisissant les images dans chacun des blocs qui sont de cardinal d.

On va utiliser ce résultat pour démontrer le lemme suivant.

Lemme 1 (Dixon [3])**.** *La proportion i_n de couples $(x, y) \in \mathfrak{S}_n^2$ qui engendrent un groupe imprimitif est au plus $n/2^{\frac{n}{4}}$.*

Remarque : Comme $p_n = t_n - i_n$ et $n/2^{\frac{n}{4}} = O(n^{-2})$, le lemme 1 donne que $p_n = 1 - \frac{1}{n} + O(\frac{1}{n^2})$, ce qui montre donc la deuxième partie du théorème 1.

Démonstration. Le nombre de façons de partitionner n en m sous-ensembles contenant chacun d éléments est donné par

$$\frac{n!}{(d!)^m m!}.$$

Ainsi, l'équation (3) montre que le nombre de couples $(x, y) \in \mathfrak{S}_n^2$ qui engendrent un groupe imprimitif est

$$(n!)^2 i_n \leq \sum \frac{(m!)^2 t_m (d!)^{2m} n!}{(d!)^m m!} \leq \sum n! m! (d!)^m \tag{4}$$

car $t_m \leq 1$. Ici, la sommation porte sur tous les entiers m et d tels que $md = n$ avec $1 < m < n$. Mais

$$\begin{aligned} \frac{m!(d!)^m}{n!} = m!(d!)^m \prod_{i=1}^{m} \frac{(id-d)!}{(id)!} = \prod_{i=1}^{m} i \frac{(id-d)!d!}{(id)!} = \prod_{i=1}^{m} \frac{i}{\binom{id}{d}} = \prod_{i=1}^{m} \prod_{j=1}^{d-1} \frac{d-j}{id-j} \\ \leq \prod_{i=1}^{m} i^{-d+1} = (m!)^{-d+1} \leq \left(2^{m/2}\right)^{-d/2} = 2^{-n/4} \end{aligned} \tag{5}$$

car $m \geq 2$ et $d \geq 2$. Puisqu'il y a moins de n différentes valeurs de m, on peut finalement conclure à partir des deux dernières inégalités (4) et (5) que

$$i_n \leq \sum \frac{m!(d!)^m}{n!} \leq n \cdot 2^{-n/4},$$

comme affirmé.

Cela prouve le lemme 1 et la preuve du théorème 1 est ainsi complétée. □

4 Le théorème de Jordan

Pour pouvoir déduire le théorème 2 du théorème 1, il est d'abord nécessaire d'introduire un théorème dû à Jordan.

Théorème 3. *[7, Theorem 13.9] Un sous-groupe primitif de $\mathfrak{S}_n$ est égal à $\mathfrak{S}_n$ ou $\mathfrak{A}_n$ quand il contient au moins une permutation qui est un q-cycle pour q un entier premier et $q \leq n - 3$.*

Pour démontrer ce théorème, on va devoir introduire plusieurs lemmes expliqués dans [7]. On introduira aussi les notations suivantes :

- Pour G un groupe de permutations sur Ω et $\Delta \subsetneq \Omega$ un bloc fixé par G. Toute permutation g de G en induit une sur Δ notée g^Δ. L'ensemble des g^Δ formé par tous les éléments de G est appelé constituant de G et noté G^Δ.
- Pour G un groupe de permutations sur Ω et $\Delta \subsetneq \Omega$, les permutations de G qui fixent chaque point de Δ forment un sous-groupe de G noté G_Δ.

— l'action d'un élément g sur un ensemble Δ sera parfois noté Δ^g.

Lemme 2. *[7, Proposition 6.1] Si Ψ et Ψ' sont des blocs de G alors leur intersection est aussi un bloc de G.*

En effet si $(g(\Psi \cap \Psi')) \cap (\Psi \cap \Psi') \neq \emptyset$ alors $(g(\Psi)) \cap (\Psi) \neq \emptyset$ donc $g(\Psi) = \Psi$ et de même pour Ψ' donc $g(\Psi \cap \Psi') = \Psi \cap \Psi'$.

Lemme 3. *[7, Theorem 8.4] Soit G un groupe transitif sur Ω. De plus, soit $U \leq G$ et soit Δ une orbite de U. Si U^Δ est primitif sur Δ et si $|\Omega| < 2|\Delta|$, alors G est primitif sur Ω.*

Démonstration. Soit $\alpha \in \psi$, où ψ est un bloc de G. Nous voulons montrer que ψ est trivial.

Ψ est aussi un bloc de U. Soit $\alpha^U = \Delta$, un bloc fixé de U. Alors, par le lemme précédent, $\Delta \cap \psi$ est un bloc de U, donc aussi de U^Δ. Il contient α. Par la primitivité de U^Δ, on en déduit que $\Delta \cap \psi$ est trivial, donc soit $\Delta \cap \psi = \Delta$, soit $\Delta \cap \psi = \{\alpha\}$.

Si $\Delta \cap \psi = \Delta$, alors $\Delta \subseteq \psi$, donc $\psi = \Omega$ car $|\Delta|$ divise $n = |\Omega|$ car G est transitif et $|\psi| \geq |\Delta| > |\Omega|/2$. Supposons maintenant que $\Delta \cap \psi = \{\alpha\}$. Pour tout $g \in G$, le bloc $\Delta \cap \psi^g$ est un bloc de U^Δ. S'il est égal à U^g, on conclut comme précédemment que $\psi^g = \Omega$ donc $\psi = \Omega$. Supposons maintenant que le bloc $\Delta \cap \psi^g$ est au plus un point pour chaque $g \in G$. (Il n'y a pas d'autres possibilités à cause de la primitivité de U^Δ.) Le nombre de ψ^g différents est alors supérieur à $|\Delta|$ et donc à $n/2$ strictement. Comme c'est un diviseur de n, il est donc égal à n. Donc $|\psi| = 1$. Dans tous les cas, ψ est un bloc trivial. Par conséquent, G est primitif. □

On déduit de cela le lemme suivant.

Lemme 4. *[7, Proposition 8.5] Soit G un groupe transitif sur Ω tel que $G = \langle C,\ D\rangle$ avec C primitif sur $\Gamma \subsetneq \Omega$ et $C \leq G_{\Omega\setminus\Gamma}$, et D primitif sur $\Delta \subsetneq \Omega$ et $D \leq G_{\Omega\setminus\Delta}$. Alors G est primitif sur Δ.*

Démonstration. En effet comme G est transitif sur Ω on a que tous les points de Ω sont reliés par une permutation de G. Or C fixe les points en dehors de Γ et D ceux en dehors de Δ donc on a forcément que $\Gamma \cap \Delta \neq \emptyset$ et $\Gamma \cup \Delta = \Omega$. On a donc que $|\Gamma| > n/2$ ou que $|\Delta| > n/2$. Donc G est primitif sur Ω. □

Lemme 5. *[7, Theorem 7.3] Si $\Delta \subsetneq \Omega$ et $\alpha \in \Omega$, alors $\psi = \cap_{\alpha \in \Delta^g} \Delta^g$ est un bloc du groupe transitif G.*

Démonstration. Soit $h \in G$ et $\psi \cap \psi^g \neq \emptyset$. Tout d'abord, soit $\alpha \in \psi^h$. Alors $\alpha \in \Delta^g$ implique $\alpha \in \Delta^{gh}$, on a donc $\psi \subsetneq \psi^h$. Comme $|\psi| = |\psi^h|$ on a $\psi = \psi^h$. Maintenant soit $\beta \in \psi \cap \psi^h$. Comme G est transitif, il existe un $k \in G$ tel que $\alpha^k = \beta$. On a donc que α appartient à $\psi^{k^{-1}}$ et à $\psi^{hk^{-1}}$. Avec ce qui vient d'être montré, on a alors que $\psi = \psi^{k^{-1}} = \psi^{hk^{-1}}$. En appliquant k on a donc finalement que $\psi = \psi^h$ et ψ est donc un bloc de G. □

De ce théorème, on peut en déduire, si G est primitif, que $\alpha = \cap_{\alpha \in \Delta^g} \Delta^g$ si $\Delta \subsetneq \Omega$ et $\alpha \in \Omega$ et donc en déduire le lemme suivant.

Lemme 6. *[7, Theorem 8.1] Soit $\Delta \subsetneq \Omega$. Si G est primitif sur Ω alors pour tout couple $(\alpha, \beta) \in \Omega^2$ avec $\alpha \neq \beta$, il existe $g \in G$ tel que $\alpha \in \Delta^g$ et $\beta \notin \Delta^g$.*

Lemme 7. *[7, Theorem 13.1] Soit G un groupe primitif agissant sur Ω. Si, de plus, G_Δ est primitif sur Γ, alors G est même 2-primitif.*

Démonstration. Nous prouvons ce lemme par récurrence sur $|\Delta|$. Pour $|\Delta| = 1$, l'assertion est triviale. Soit maintenant $|\Delta| > 1$.

(a) Supposons d'abord que $2|\Delta| \leq |\Omega|$. Cela implique $2|\Gamma| \geq |\Omega|$, et donc pour tout $g \in G$ nous avons $\Gamma \cap \Gamma^g \neq \emptyset$. Soient $\alpha, \beta \in \Delta$ distincts. En raison de la primitivité de G_Δ, il existe un $g \in G_\Delta$ tel que $\alpha^g = \beta$ et $\beta^g \notin \Delta$ par le lemme 6. Puisque $\Gamma \cap \Gamma^g \neq \emptyset$, le groupe $H = \langle G_\Delta, g^{-1} G_\Delta g \rangle$ est transitif sur $\Gamma \cup \Gamma^g$ car G_Δ est transitif sur Γ et $\langle G_\Delta, g^{-1} G_\Delta g \rangle$ est transitif sur Γ^g. $\Delta' = \Delta \cap \Delta^g$ est l'ensemble des points qui sont fixés par tous les éléments de H. Puisque $\alpha \in \Delta'$, nous avons $1 \leq |\Delta'|$, et puisque $\beta \notin \Delta'$, nous avons $|\Delta'| < |\Delta|$. Par l'hypothèse de récurrence on obtient la 2-transitivité de G. Si G_Δ est primitif, alors d'après le lemme 4, H est aussi primitif. Le même raisonnement montre la 2-primitivité de G.

(b) On suppose maintenant que $2|\Delta| \geq |\Omega|$. Soient $\alpha, \beta \in \Gamma$. Par le lemme 6, il existe un $g \in G_\Delta$ tel que $\alpha \in \Gamma^g$ et $\beta^g \notin \Gamma$. Nous avons $\alpha \in \Gamma \cap \Gamma^g$, donc $\Gamma^g \cap \Gamma \neq \emptyset$ et encore $H = \langle G_\Delta, g^{-1} G_\Delta g \rangle$ est transitif sur $\Gamma \cup \Gamma^g$. Comme $2|\Gamma| \leq |\Omega|$, on a $\Gamma \cup \Gamma^g \subsetneq \Omega$ de plus $\Gamma \neq \Gamma^g$ donne que $\Gamma \cup \Gamma^g \subsetneq \Gamma$. Maintenant, on peut à nouveau utiliser l'hypothèse de récurrence comme auparavant, et obtenir la 2-primitivité ou la 2-transitivité de G (selon que G_Δ soit primitif ou non). □

Lemme 8. *[7, Theorem 9.1] Soit G un groupe transitif sur Ω et $\alpha \in \Omega$. Alors G est k-fois transitif si et seulement si G_α est k-fois transitif sur $\Omega \setminus \{\alpha\}$. Si G est k-fois transitif sur Ω et $\Delta \subsetneq \Omega$ avec $|\Delta| = d < k$, alors G_Δ est $(k-d)$-fois transitif sur $\Omega \setminus \Delta$.*

Lemme 9. *[7, Theorem 13.2] Si G est primitif sur Ω et G_Δ est primitif sur $\Omega \setminus \Delta = \Gamma$, et si de plus $1 < |\Gamma| = m < n = |\Omega|$, alors G est $(n - m + 1)$-primitif.*

Démonstration. On prouve ce lemme par récurrence sur $n - m = |\Delta|$. Pour $n - m = 1$, c'est trivial. Supposons maintenant $n - m > 1$. Soit $\delta \in \Delta$. Alors $\Gamma \subsetneq \Omega \setminus \{\delta\}$ et G est 2-primitif (par le lemme 7). On a donc que G_δ est primitif sur $\Omega \setminus \{\delta\}$, et par hypothèse de récurrence on a que G_δ est$(n-m)$-primitif. Comme G est transitif on peut conclure avec le lemme 8. □

En particulier si $m = 2$ on a que G est $(n-1)$-fois transitif et si $m = 3$ on a que G est $(n-2)$-fois transitif et on a donc le lemme suivant.

Lemme 10. *[7, Theorem 13.3] Un groupe primitif qui contient une transposition est le groupe symétrique. Un groupe primitif qui contient un 3-cycle est soit le groupe symétrique soit le groupe alterné.*

Lemme 11. *[7, Theorem 9.4] Soit G k-fois transitif sur Ω et soit $\Gamma \subseteq \Omega$, $|\Gamma| = k$. Soit le sous-groupe $U \leq G_\Gamma$ tel que U est conjugué dans G_Γ à tous les sous-groupes de G_Γ qui sont conjugués à U dans G. Alors le normalisateur $N(U)$ de U est k-fois transitif sur l'ensemble des points fixés par U.*

Lemme 12. *[7, Theorem 11.2] Soit N un sous-groupe normal régulier de G sur Ω. Soit $\alpha \in \Omega$. On fait agir G_α sur N par conjugaison et l'on voit cette action comme l'action d'un groupe A de permutations sur $N \setminus \{id\}$. Alors l'action de G_α sur $\Omega \setminus \{\alpha\}$ correspond à l'action de A sur $N \setminus \{id\}$. En effet les permutations n de N sont en bijection avec les point de $\Omega \setminus \{\alpha\}$ par l'application $n \mapsto \alpha^n$.*

Démonstration. Soit $\gamma, \delta \in \Omega \setminus \{\alpha\}$ et soit $g \in G_\alpha$ tel que $\gamma^g = \delta$. De plus soit $c, d \in N \setminus \{id\}$ les permutations correspondantes à γ et δ, on a donc que $\alpha^c = \gamma$ et $\alpha^d = \delta$. Alors $d^{-1}g^{-1}cg \in N$ comme N est un sous-groupe normal. De plus $\alpha^{d^{-1}g^{-1}cg} = \alpha$. Donc $d^{-1}g^{-1}cg = id$ par la régularité de N et on a bien finalement que $g^{-1}cg = d$. □

On a maintenant tous les outils nécessaires pour démontrer le théorème 3.

Démonstration du théorème 3. Supposons que G contienne le cycle $g = (1\ 2\ \ldots\ p)$. Soit $\Delta = \{p+1, \ldots, n\}$ l'ensemble des k points restants. Alors le sous-groupe $\langle g \rangle$ est un p-sous-groupe de Sylow de G_Δ.

D'après le lemme 9, G agit k-transitivement sur Ω. Par conséquent, d'après le théorème lemme 11, le normalisateur $N = N(\langle g \rangle)$ agit également k-transitivement sur Ω. On a donc $N^\Delta = S^\Delta$. Soit $\alpha \in \Gamma$. Alors $N = N_\alpha G_\Delta$, et donc $(N_\alpha)^\Delta = N^\Delta$.

Pour le prouver, notons que $N_\alpha G_\Delta \subseteq N$. Soit maintenant $n \in N$. Puisque Γ est fixé par N, il s'ensuit que $\alpha^n = \beta \in \Gamma$. En raison de la transitivité de G_Δ sur Γ, il existe un $h \in G_\Delta$ tel que $\alpha^h = \beta$. Alors $n' = nh^{-1} \in N_\alpha$, et donc $n = n'h \in N_\alpha G_\Delta$.

Par le lemme 12, $N^{\Omega\setminus\Delta}$ est isomorphe à un sous-groupe du groupe des automorphismes de $\langle g \rangle$, donc abélien.

Soit $K = [N, N]$ le sous-groupe dérivé de N. Alors K a pour constituant $K^{\Omega\setminus\Delta} = 1$ et $K^\Delta = [S^\Delta, S^\Delta] = A^\Delta$. Il en résulte que G contient un cycle d'ordre 3.

Enfin, comme G est primitif et contient un 3-cycle, on conclut, par le lemme 10, que $A^\Omega \leq G$. Donc G est soit $\mathfrak{A}_n$ soit $\mathfrak{S}_n$. □

5 Démonstration du théorème 2

Rappelons qu'une permutation de $\mathfrak{S}_n$ peut être écrite (de manière unique à permutation des cycles entre eux près) comme un produit de cycles disjoints ; nous appellerons cela sa *décomposition en cycles*. Pour chaque nombre premier $q < n - 3$, nous définissons $C_{qn} \subseteq \mathfrak{S}_n$ comme l'ensemble des permutations de $\mathfrak{S}_n$ dont la décomposition en cycles contient exactement un cycle de longueur q et tous les autres cycles de longueur première avec q. Si $z \in C_{qn}$ est d'ordre h, alors q divise h et $z^{h/q}$ est un q-cycle. Ainsi, d'après le théorème 3 de Jordan, un sous-groupe primitif de $\mathfrak{S}_n$ qui contient au moins un élément de $\bigcup_q C_q$ est égal à $\mathfrak{A}_n$ ou $\mathfrak{S}_n$. Le point essentiel dans notre démonstration du Théorème 1 est de montrer que presque tous les éléments de $\mathfrak{S}_n$ sont dans $\bigcup_q C_{qn}$.

Lemme 13. *Soit $T_n = \bigcup_q C_{qn}$, où l'union est prise sur tous les nombres premiers q tels que $(\log n)^2 \leq q \leq n - 3$. Alors la proportion u_n des éléments de $\mathfrak{S}_n$ qui sont dans T_n est*

au moins

$$1 - \frac{4}{3\log\log n}$$

pour tout n suffisamment grand.

Démonstration. Nous avons besoin de deux résultats de l'article [4]. Le Theorem VI de cet article montre que, pour tous entiers a_i tels que $1 < a_1 < a_2 < \cdots < a_k < n$, la proportion des permutations dans $\mathfrak{S}_n$ dont la décomposition en cycles ne contient aucun cycle de longueurs $a_1, a_2, \ldots, a_k$ est au plus $\left(\sum_{i=1}^{k} \frac{1}{a_i}\right)^{-1}$. Le Lemma 1 de cet article montre de plus que la proportion des éléments dans S_{n-q} d'ordre premier avec q (pour un premier donné q) est $\prod_{i=1}^{\frac{n-q}{q}} \left(1 - \frac{1}{qi}\right)$. Des estimations élémentaires donnent

$$\prod_{i=1}^{\frac{n-q}{q}} \left(1 - \frac{1}{qi}\right) = \exp\left(-\frac{\log(n-q) - \log(q) + O(1)}{q}\right).$$

En effet

$$\begin{aligned}\log\left(\prod_{i=1}^{\frac{n-q}{q}} \left(1 - \frac{1}{qi}\right)\right) &= \sum_{i=1}^{\frac{n-q}{q}} \log\left(1 - \frac{1}{qi}\right) = \sum_{i=1}^{\frac{n-q}{q}} \left(-\frac{1}{qi} + O\left(\frac{1}{(qi)^2}\right)\right) \\ &= -\frac{1}{q}\left(\gamma + \log(\frac{n-q}{q}) + O(\frac{q}{n-q})\right) + O(\frac{1}{q^2}) = -\frac{1}{q}\Big(\log(\frac{n-q}{q}) + O(1)\Big).\end{aligned}$$

Donc

$$\prod_{i=1}^{\frac{n-q}{q}} \left(1 - \frac{1}{qi}\right) \geq \exp\left(-\frac{1}{\log(n)}\right)$$

pour tout n suffisamment grand et tel que $(\log n)^2 \leq q \leq n - 3$.

Une permutation est d'ordre premier avec q si et seulement si tous les cycles dans sa décomposition en cycles ont une longueur première avec q. Ainsi, d'après les deux résultats précédents et la définition de C_{qn}, on conclut que

$$u_n \geq \left(1 - \left(\sum_q \frac{1}{q}\right)^{-1}\right) \cdot \exp\left(-\frac{1}{\log(n)}\right)$$

pour tout n suffisamment grand. Ci-dessus, la somme porte sur tous les nombres premiers q tels que $(\log n)^2 \leq q \leq n - 3$.

D'autre part, il est connu ([5, Théorème 427]) que

$$\sum_p \frac{1}{p} = \log(\log(n)) + O(1)$$

où p parcourt tous les nombres premiers $1 \leq p \leq n$. Ainsi

$$\sum_q \frac{1}{q} = \log(\log(n-3)) - \log(\log(\log(n)^2)) + O(1) > \frac{4}{5}\log(\log(n))$$

pour tout n suffisamment grand. En effet $\log(\log(\log(n)^2)) = o(\log(\log(n))$ quand $n \to \infty$ et

$$\begin{aligned}\log(\log(n-3)) - \frac{4}{5}\log(\log(n)) &= \log\left(\frac{\log(n-3)}{\log(n)^{\frac{4}{5}}}\right) \\ &= \log\left(\frac{\log(n)+\log(1-\frac{3}{n})}{\log(n)^{\frac{4}{5}}}\right) \to \infty \text{ quand } n \text{ tend vers l'infini.}\end{aligned}$$

D'où l'inégalité souhaité, ce qui permet d'obtenir

$$u_n \geq \left(1 - \frac{5}{4\log(\log(n))}\right)\exp\left(-\frac{1}{\log(n)}\right).$$

Et finalement

$$u_n \geq 1 - \frac{4}{3\log(\log(n))},$$

ce qui prouve le lemme. □

Nous pouvons maintenant démontrer le théorème 2. D'après le théorème 1, la proportion des couples $(x,y) \in \mathfrak{S}_n^2$ qui engendrent un sous-groupe primitif est supérieure à $1-\frac{2}{n}$ pour tout n suffisamment grand. D'après le lemme 2, la proportion des couples $(x,y) \in \mathfrak{S}_n^2$ telles que l'un au moins des deux éléments appartient à $T_n = \bigcup_q C_{qn}$ est supérieure à $1 - \frac{16}{(3\log\log n)^2}$ pour tout n suffisamment grand.

Ainsi, par les observations faites avant le lemme 2, la proportion des couples $(x,y) \in \mathfrak{S}_n^2$ qui engendrent $\mathfrak{A}_n$ ou $\mathfrak{S}_n$ est au moins

$$1 - \frac{2}{n} - \frac{16}{(3\log\log n)^2} \geq 1 - \frac{2}{(\log\log n)^2}$$

pour tout n suffisamment grand. Cela prouve le théorème 2.

Références

[1] J. Calais, Éléments de théorie des groupes, PUF (2014).

[2] L. Comtet, Advanced Combinatorics : The Art of Finite and Infinite Expansions (1974).

[3] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.

[4] P. Erdös, P. Turin, On some problems of a statistical group-theory, *Acta Math. Acad.Sci Hung* **18** (1967), 151-163.

[5] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, Oxford, Clarendon Press, (1962).

[6] E. Netto, The theory of substitutions (reprint), *New York : Chelsea* (1964).

[7] H. Weiland, Finite Permutation Groups (1964).